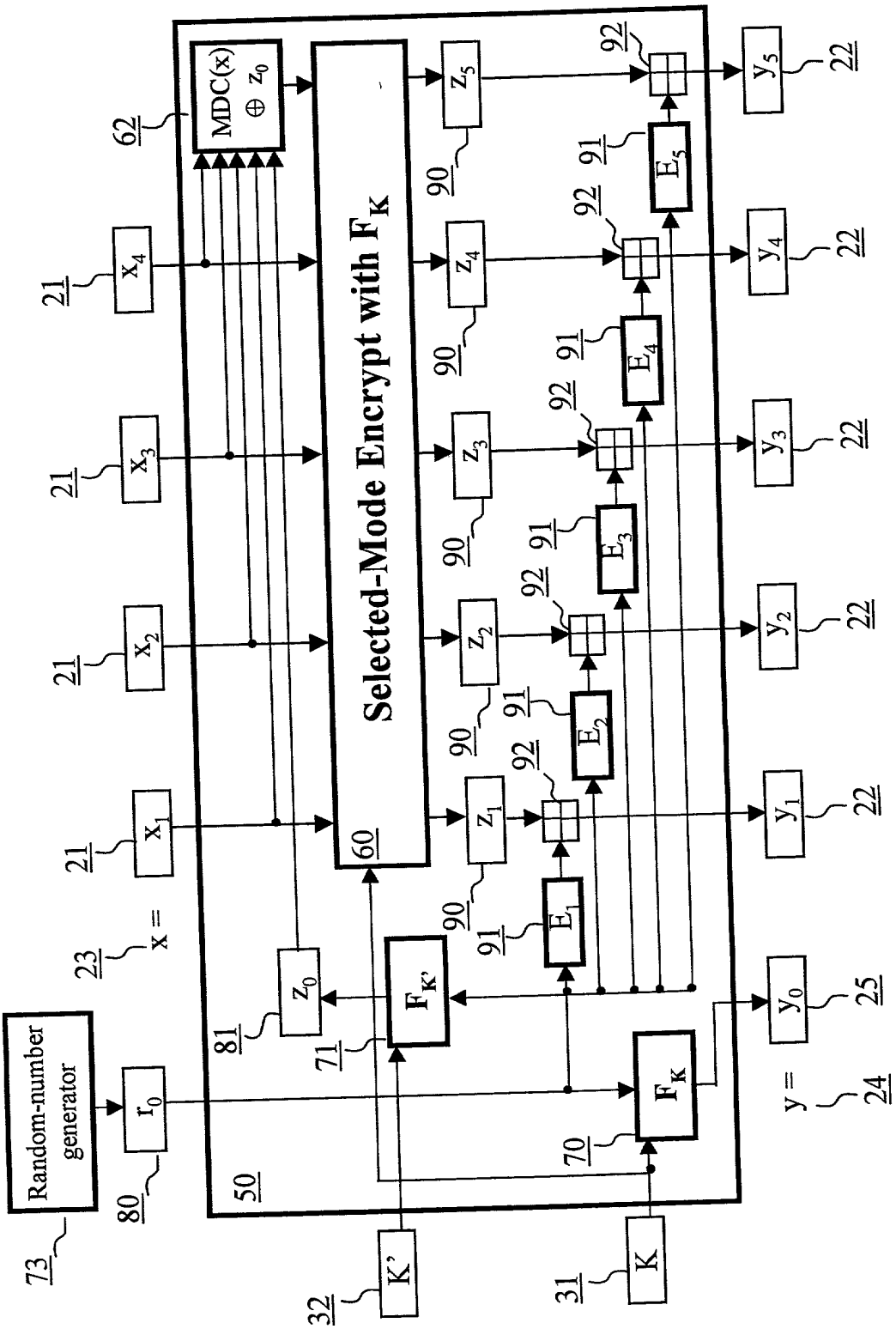

Random-number generator
73
80
r_0
50
62
MDC(x) ⊕ z_0
Selected-Mode Encrypt with F_K
60
$F_{K'}$
F_K
32
K'
31
K
x =
23
21
x_1
x_2
x_3
x_4
z_0
z_1
z_2
z_3
z_4
z_5
81
71
70
90
91
92
E_1
E_2
E_3
E_4
E_5
y_0
y_1
y_2
y_3
y_4
y_5
25
y =
24
22

FIG. 1

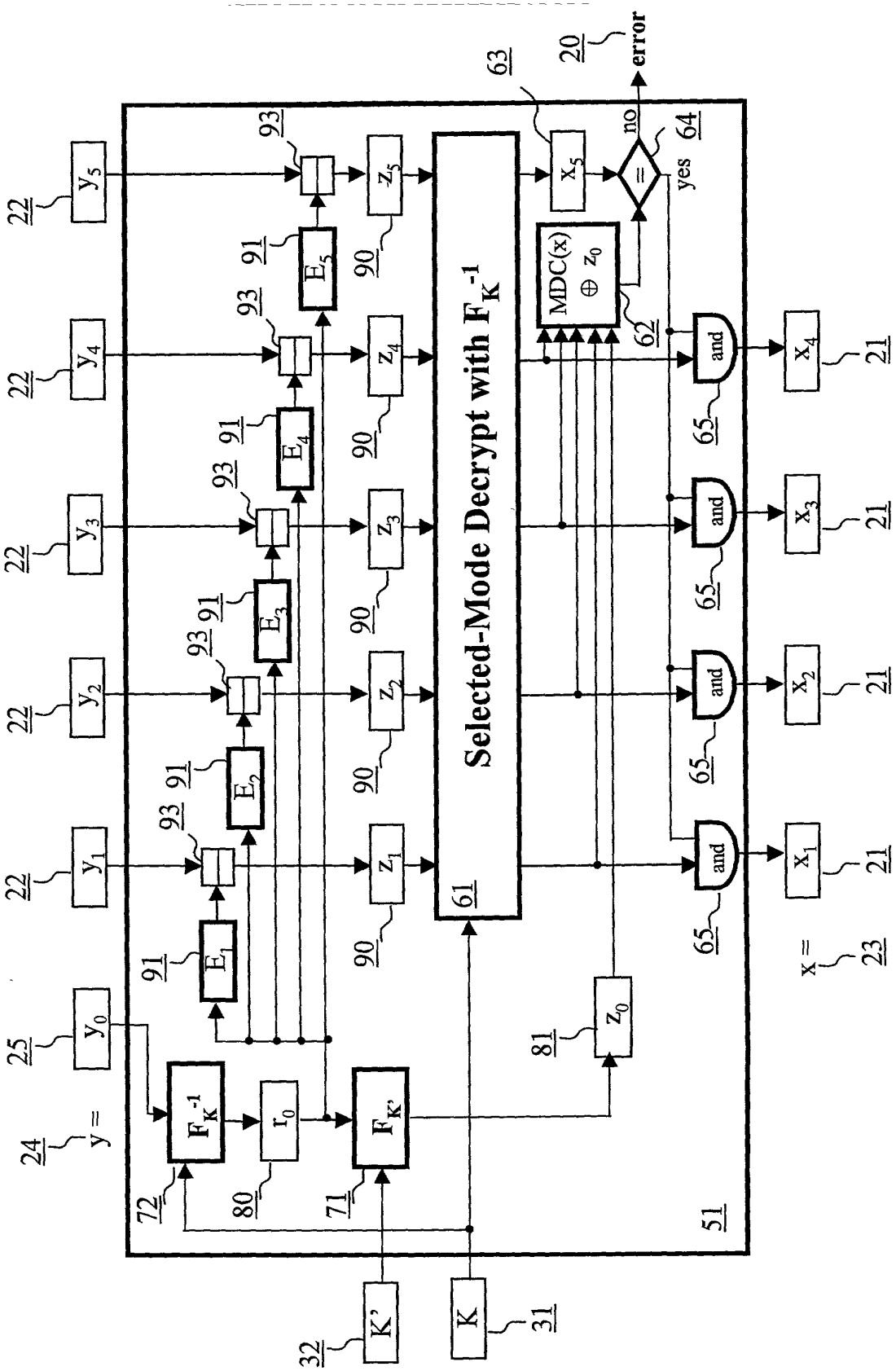

Selected-Mode Decrypt with F_K^{-1}
error
no
yes
MDC(x) ⊕ z_0
and
F_K^{-1}
$F_{K'}$
r_0
E_1
E_2
E_3
E_4
E_5
y_0
y_1
y_2
y_3
y_4
y_5
z_0
z_1
z_2
z_3
z_4
z_5
x_1
x_2
x_3
x_4
x_5
K'
K
y =
x =
20
21
22
23
24
25
31
32
51
61
62
63
64
65
71
72
80
81
90
91
93

FIG. 2

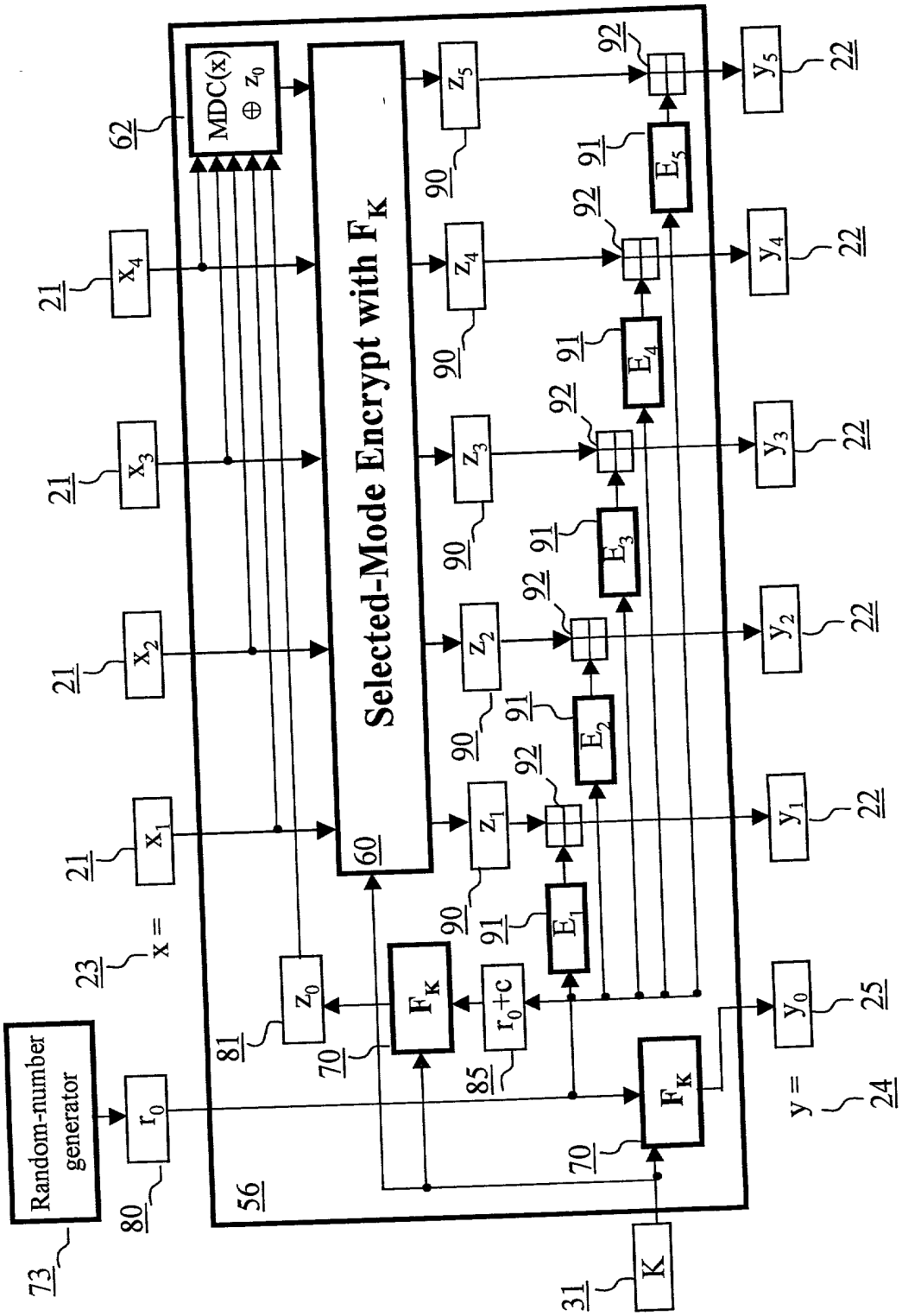
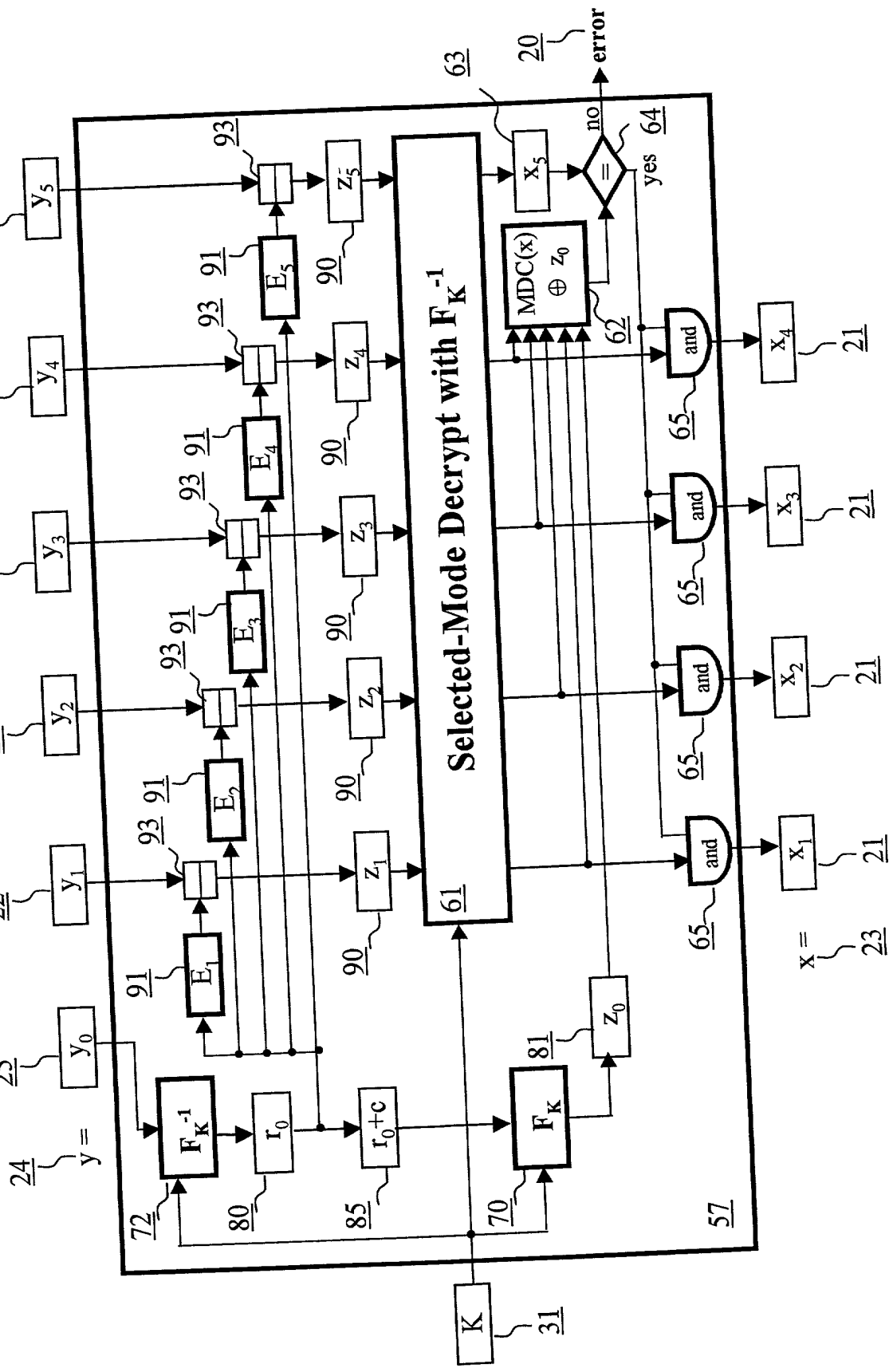

Random-number generator
73
80
r_0
81
z_0
70
F_K
85
r_0+c
E_1
E_2
E_3
E_4
E_5
91
92
90
z_1
z_2
z_3
z_4
z_5
MDC(x) $\oplus$ z_0
62
Selected-Mode Encrypt with F_K
60
56
21
x_1
x_2
x_3
x_4
23
x =
y_0
y_1
y_2
y_3
y_4
y_5
22
25
y =
24
31
K

FIG. 3

FIG. 4


Selected-Mode Decrypt with F_K^{-1}
error
no
yes
MDC(x) ⊕ z_0
and
F_K^{-1}
F_K
r_0
r_0+c
E_1
E_2
E_3
E_4
E_5
y_0
y_1
y_2
y_3
y_4
y_5
z_0
z_1
z_2
z_3
z_4
z_5
x_1
x_2
x_3
x_4
x_5
K
y =
x =
57
61
62
63
64
65
70
72
80
81
85
90
91
93
20
21
22
23
24
25
31

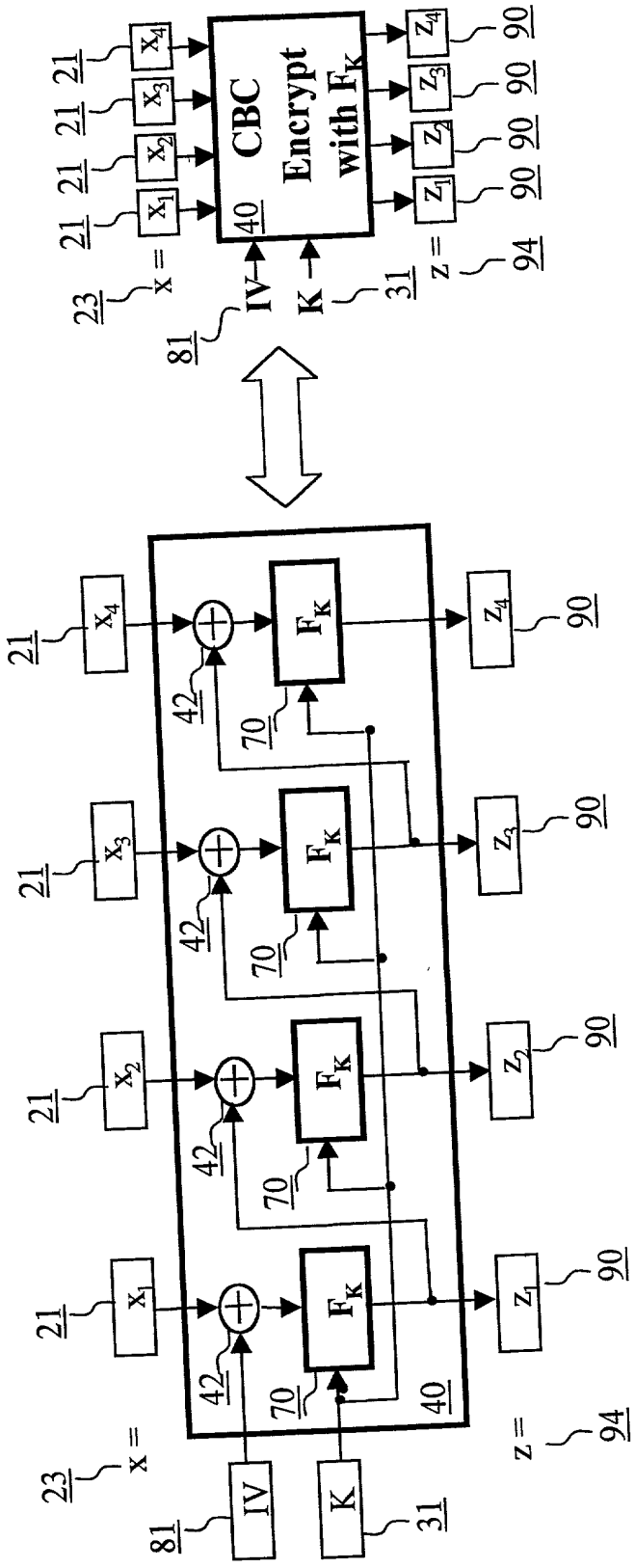

CBC
Encrypt
with F_K
IV
K
x =
z =
F_K
x_1
x_2
x_3
x_4
z_1
z_2
z_3
z_4
21
23
31
40
42
70
81
90
94

FIG. 5

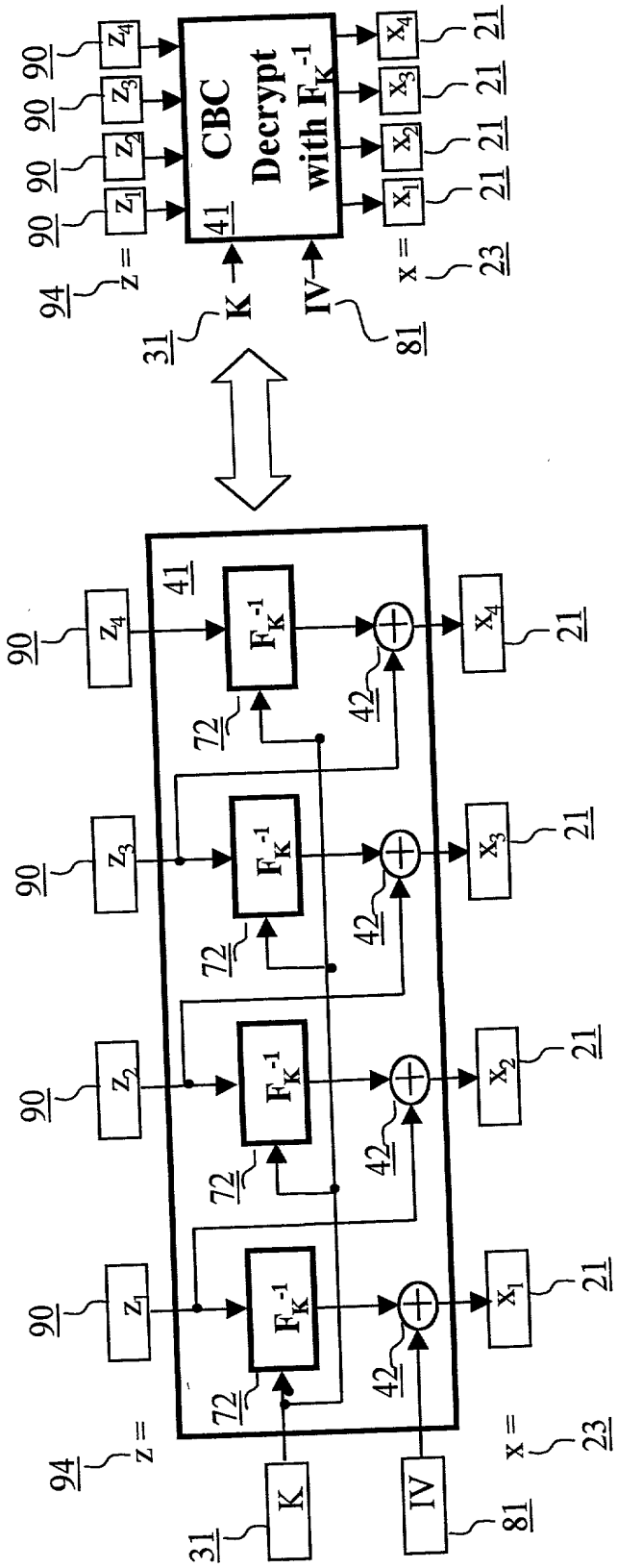

CBC
Decrypt
with F_K^{-1}
41
90
z_4
z_3
z_2
z_1
94
z =
31
K
IV
81
x =
23
x_4
x_3
x_2
x_1
21
F_K^{-1}
72
42

FIG. 6

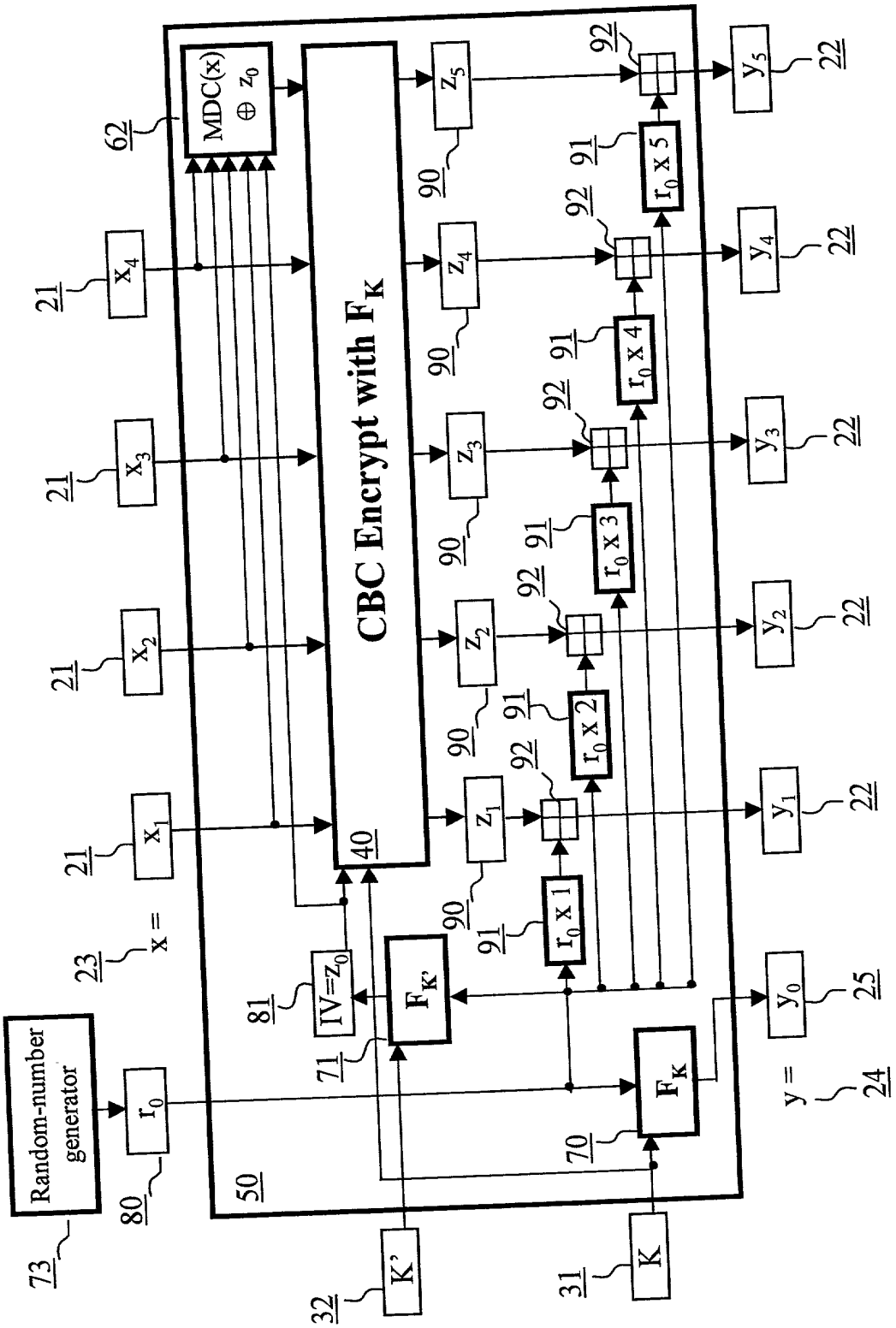

CBC Encrypt with F_K
MDC(x) ⊕ z_0
Random-number generator
r_0
IV=z_0
$F_{K'}$
F_K
K'
K
x =
y =
x_1
x_2
x_3
x_4
z_1
z_2
z_3
z_4
z_5
y_0
y_1
y_2
y_3
y_4
y_5
r_0 x 1
r_0 x 2
r_0 x 3
r_0 x 4
r_0 x 5
21
22
23
24
25
31
32
40
50
62
70
71
73
80
81
90
91
92

FIG. 7

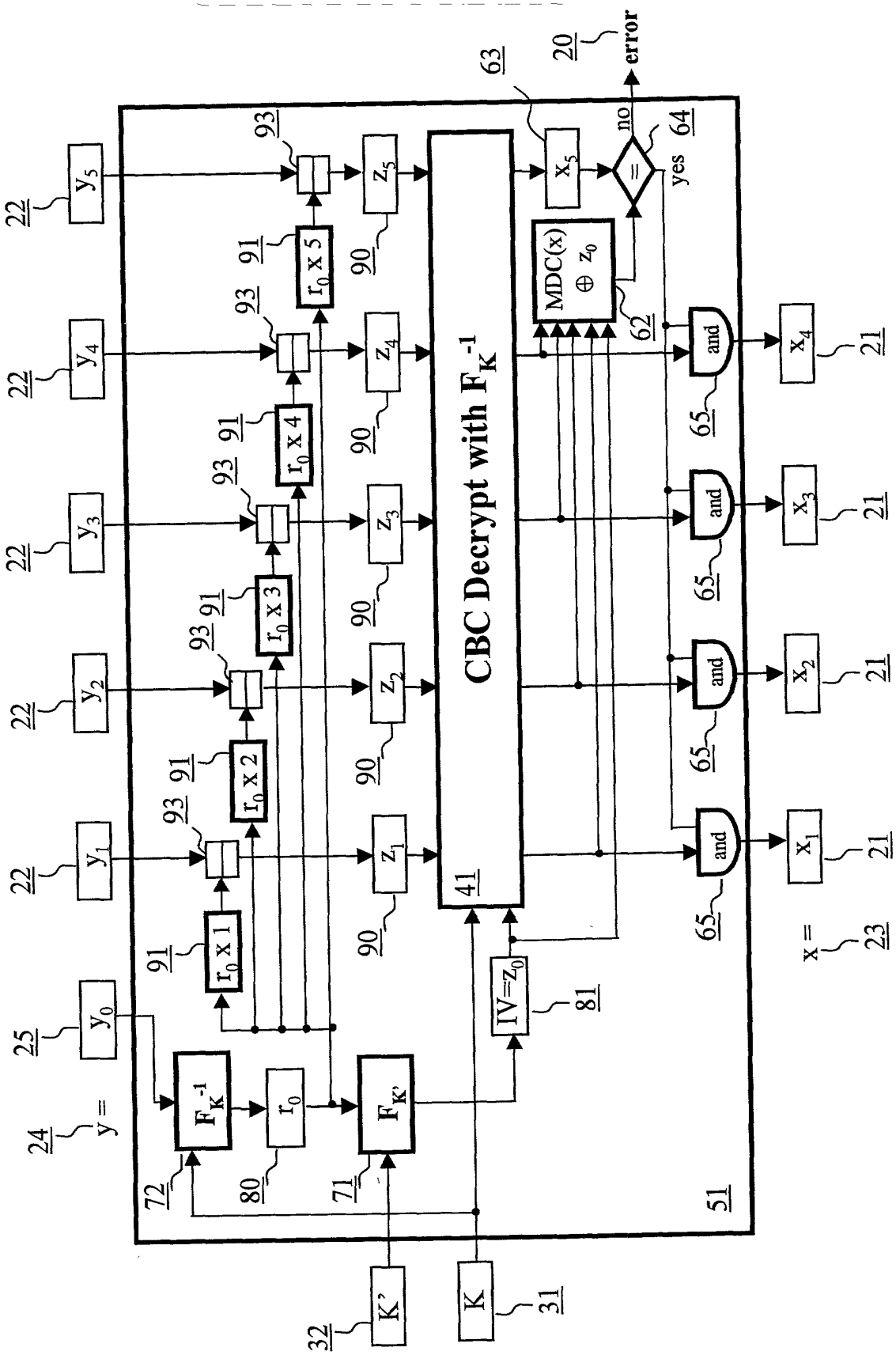
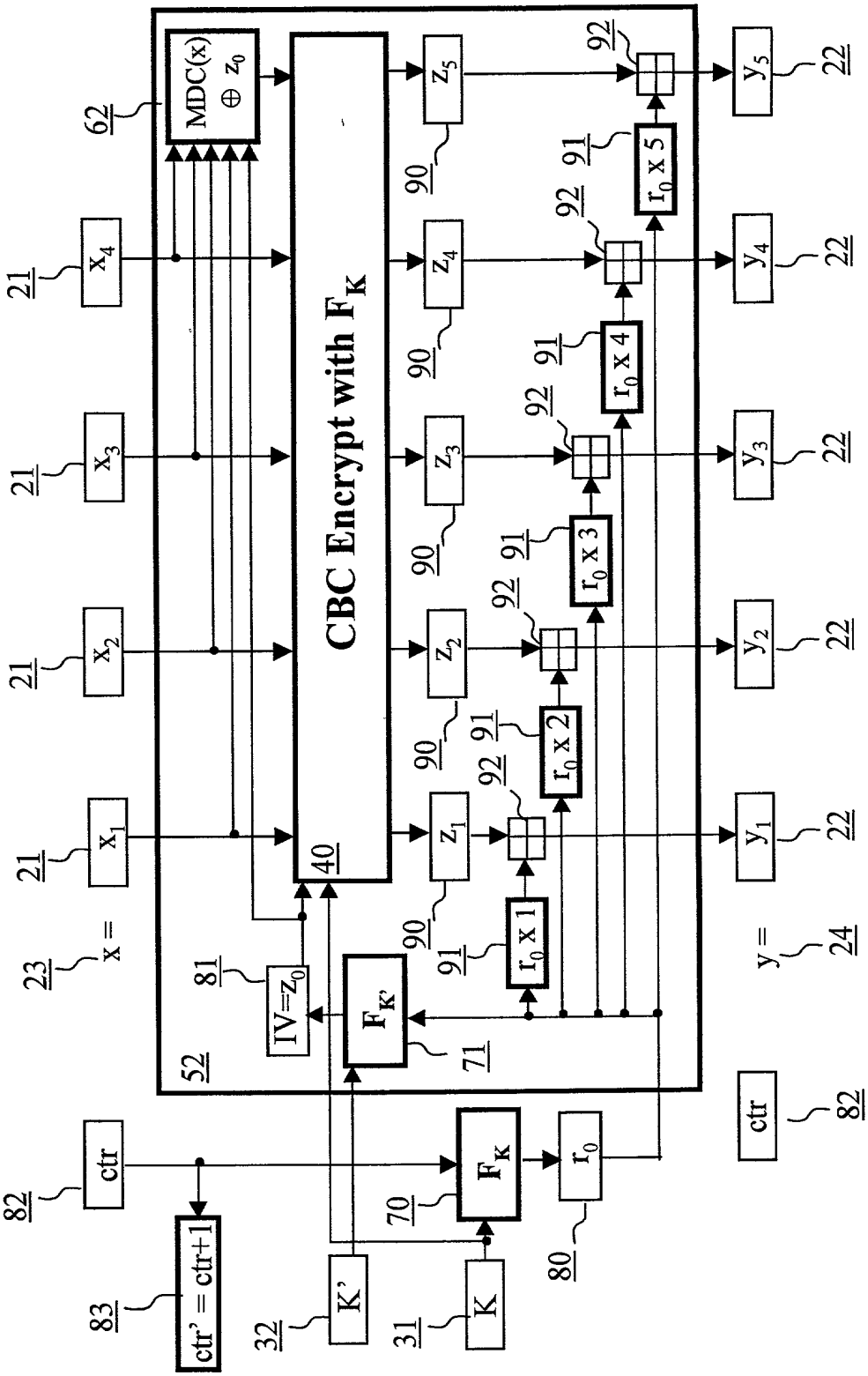

error
20
63
64
no
yes
=
MDC(x) ⊕ z0
62
CBC Decrypt with FK-1
41
IV=z0
81
FK-1
FK'
r0
72
80
71
51
K'
32
K
31
y=
24
25
y0
x=
23
22
y5
y4
y3
y2
y1
z5
z4
z3
z2
z1
90
93
91
r0 x 5
r0 x 4
r0 x 3
r0 x 2
r0 x 1
and
65
x5
x4
x3
x2
x1
21

FIG. 8

FIG. 9


CBC Encrypt with F_K
MDC(x) ⊕ z_0
x_1
x_2
x_3
x_4
z_1
z_2
z_3
z_4
z_5
y_1
y_2
y_3
y_4
y_5
r_0 x 1
r_0 x 2
r_0 x 3
r_0 x 4
r_0 x 5
IV=z_0
$F_{K'}$
F_K
r_0
ctr
ctr' = ctr+1
K'
K
x =
y =
40
52
62
70
71
80
81
82
83
90
91
92
21
22
23
24
31
32

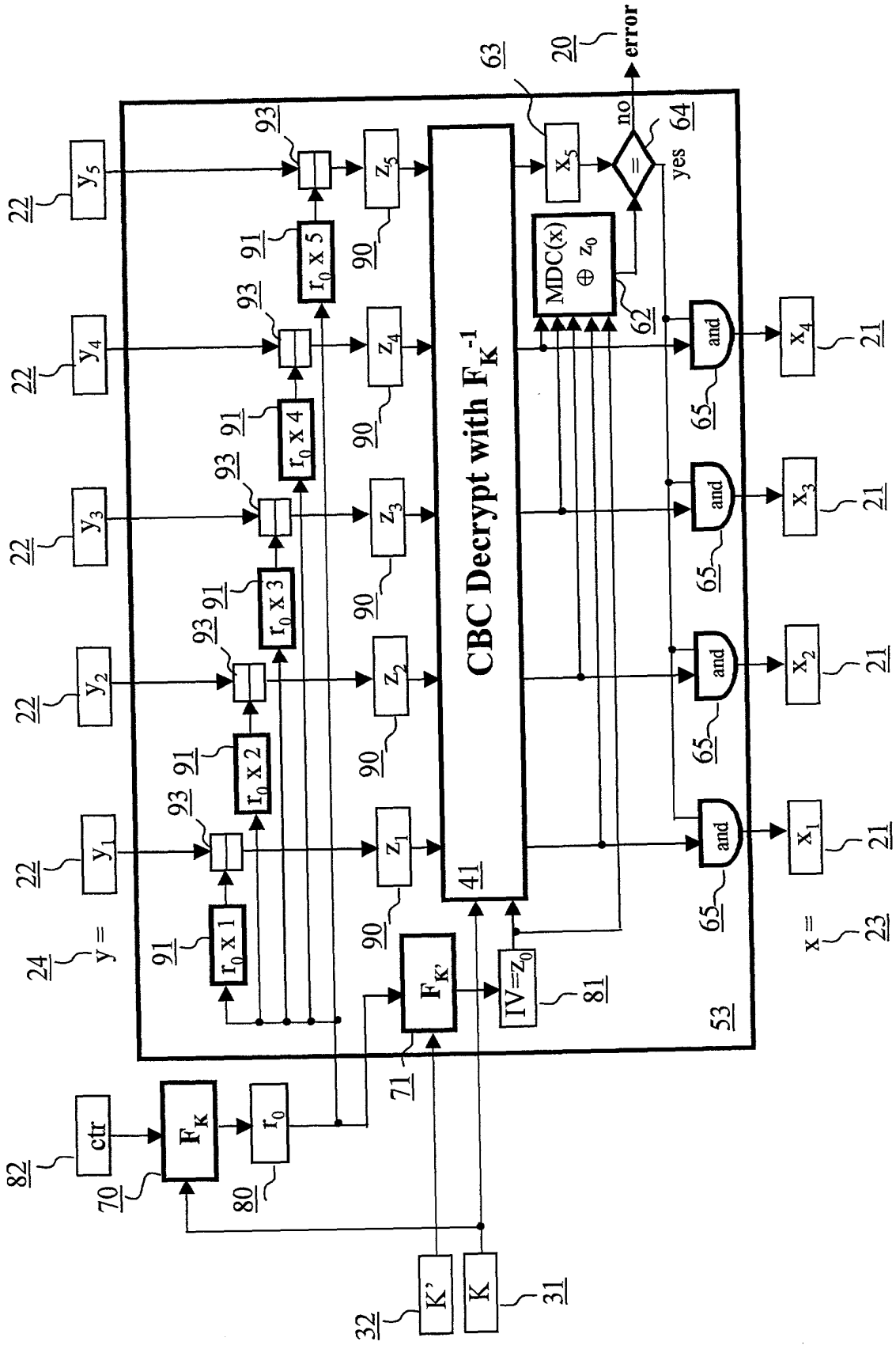

CBC Decrypt with F_K^{-1}
error
no
yes
=
MDC(x) ⊕ z_0
and
F_K
$F_{K'}$
ctr
r_0
r_0 x 1
r_0 x 2
r_0 x 3
r_0 x 4
r_0 x 5
IV=z_0
K
K'
y =
x =
20
21
22
23
24
31
32
41
53
62
63
64
65
70
71
80
81
82
90
91
93

FIG. 10

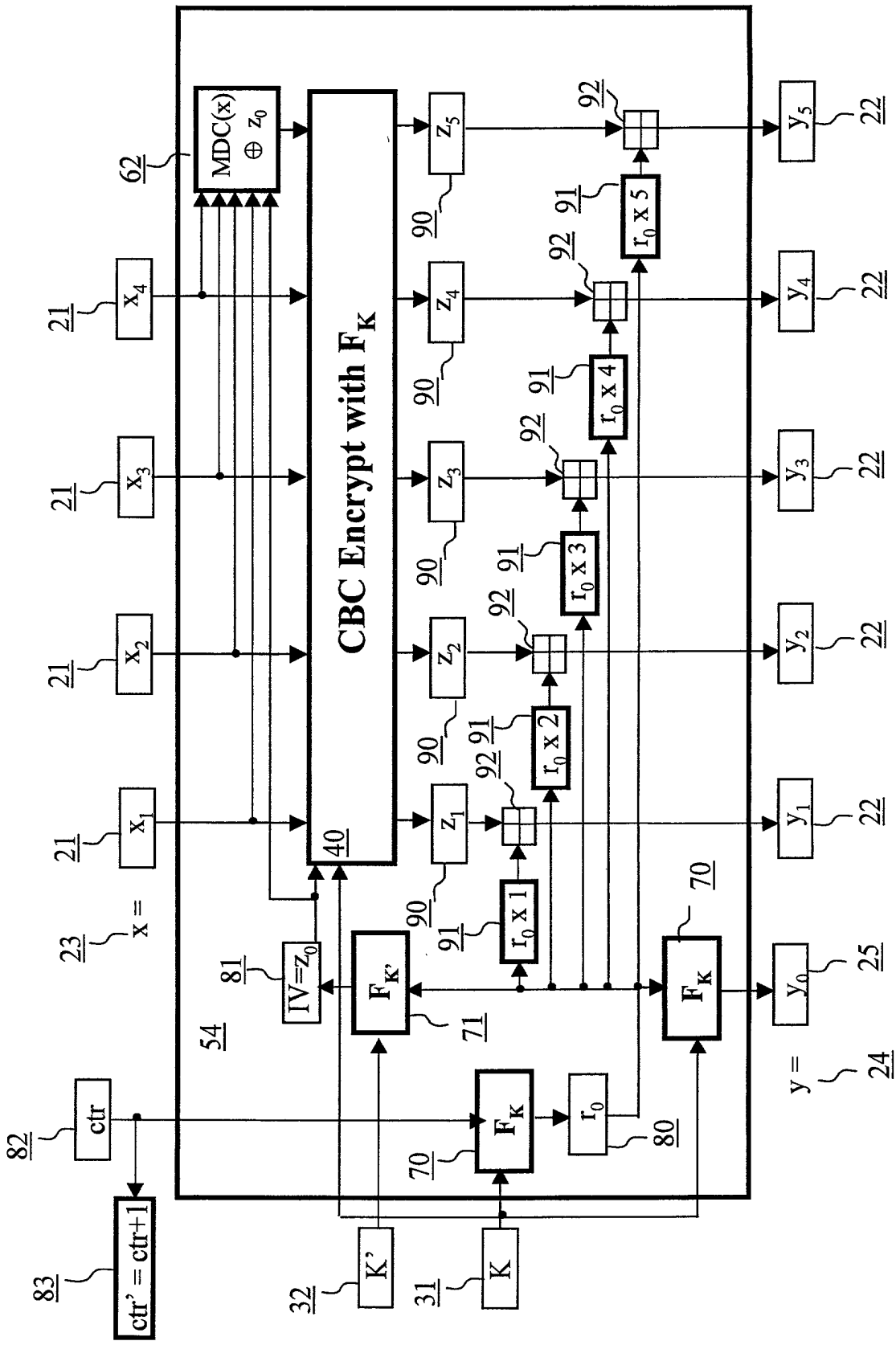

CBC Encrypt with F_K
MDC(x) ⊕ z_0
62
40
21
x_1
x_2
x_3
x_4
23
x =
z_1
z_2
z_3
z_4
z_5
90
92
91
r_0 x 1
r_0 x 2
r_0 x 3
r_0 x 4
r_0 x 5
y_0
y_1
y_2
y_3
y_4
y_5
22
25
y =
24
81
IV=z_0
54
$F_{K'}$
71
70
F_K
r_0
80
82
ctr
83
ctr' = ctr+1
32
K'
31
K

FIG. 11

FIG. 12

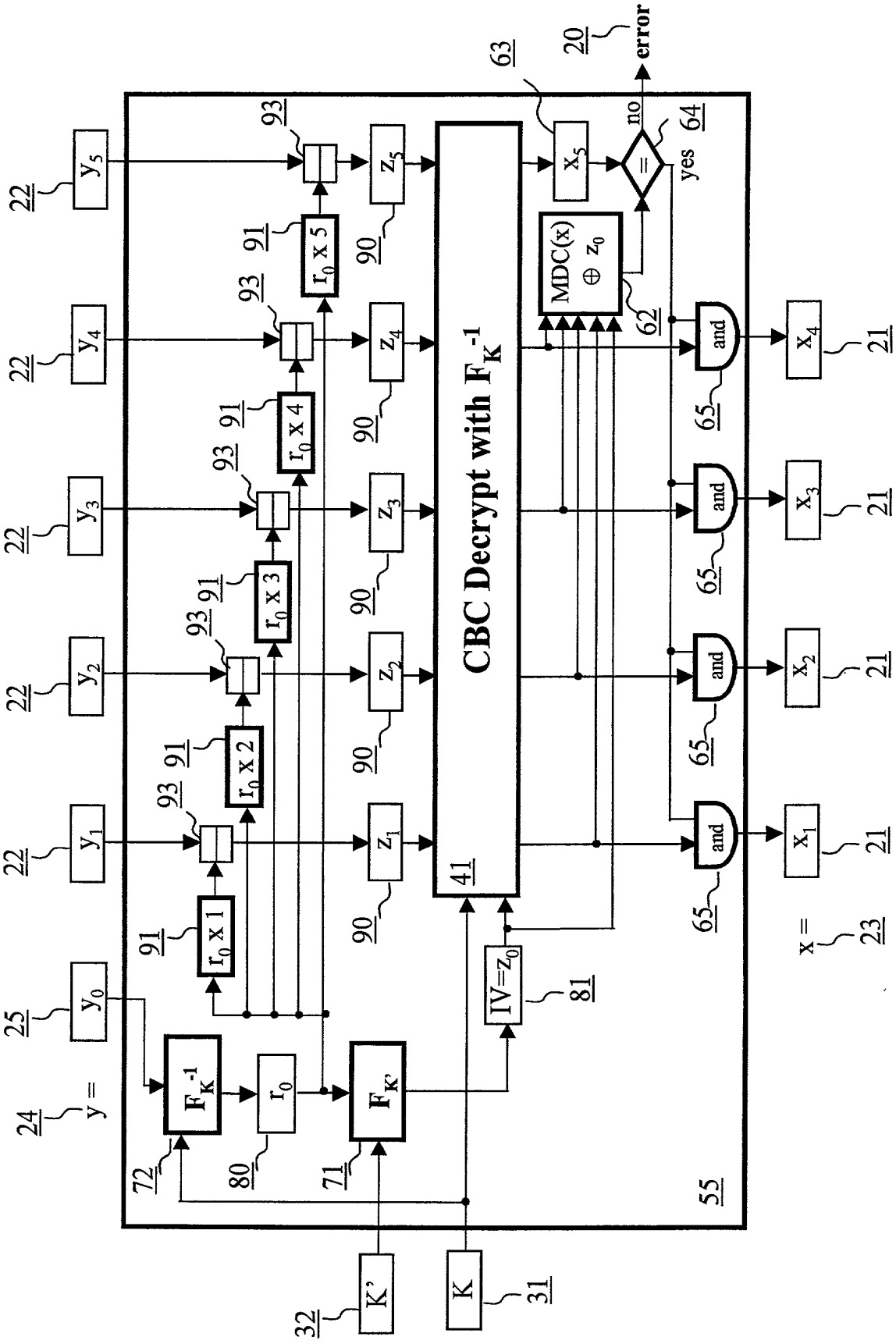

CBC Decrypt with F_K^{-1}
error
no
yes
MDC(x) ⊕ z_0
IV=z_0
F_K^{-1}
$F_{K'}$
r_0
r_0 x 1
r_0 x 2
r_0 x 3
r_0 x 4
r_0 x 5
and
y =
x =
K'
K
20
21
22
23
24
25
31
32
41
55
62
63
64
65
71
72
80
81
90
91
93

FIG. 13

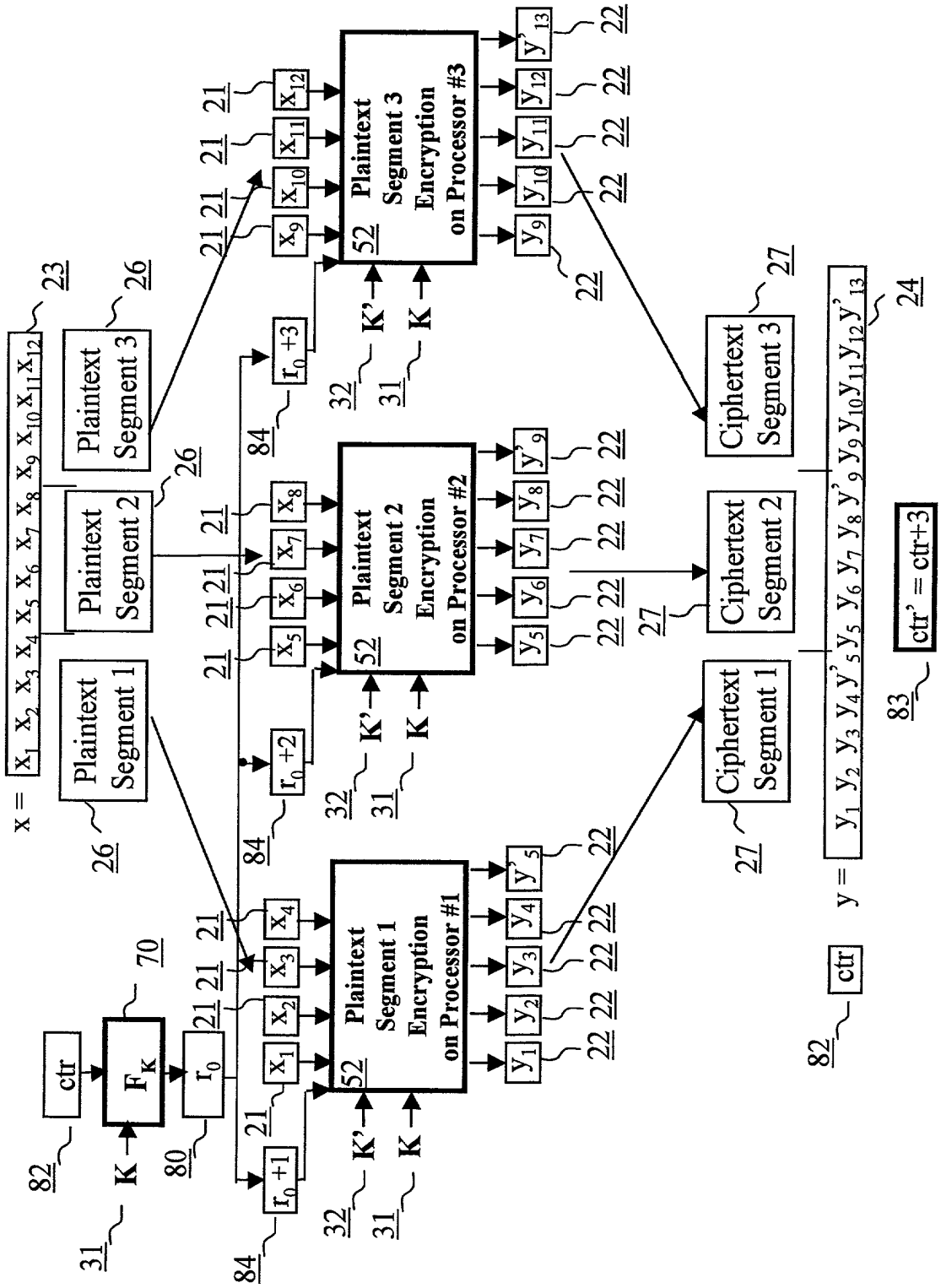
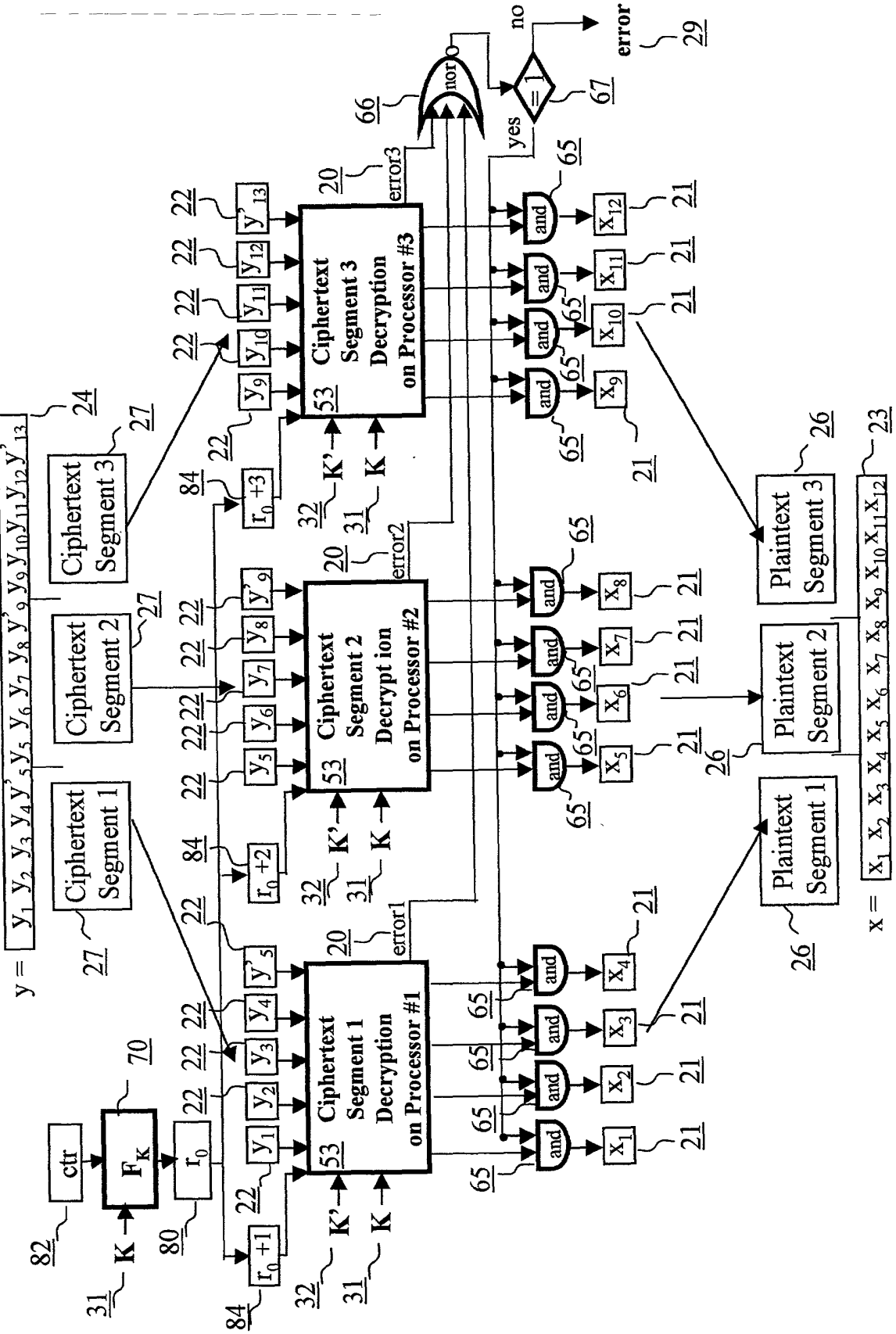

x = x1 x2 x3 x4 x5 x6 x7 x8 x9 x10 x11 x12
Plaintext Segment 1
Plaintext Segment 2
Plaintext Segment 3
Plaintext Segment 1 Encryption on Processor #1
Plaintext Segment 2 Encryption on Processor #2
Plaintext Segment 3 Encryption on Processor #3
ctr
FK
r0
r0+1
r0+2
r0+3
K
K'
Ciphertext Segment 1
Ciphertext Segment 2
Ciphertext Segment 3
y = y1 y2 y3 y4 y'5 y5 y6 y7 y8 y'9 y9 y10 y11 y12 y'13
ctr' = ctr+3

FIG. 14


y = y1 y2 y3 y4 y'5 y5 y6 y7 y8 y'9 y9 y10 y11 y12 y'13
Ciphertext Segment 1
Ciphertext Segment 2
Ciphertext Segment 3
Ciphertext Segment 1 Decryption on Processor #1
Ciphertext Segment 2 Decrypt ion on Processor #2
Ciphertext Segment 3 Decryption on Processor #3
ctr
FK
K
K'
r0
r0+1
r0+2
r0+3
error1
error2
error3
nor
yes
no
=1
error
Plaintext Segment 1
Plaintext Segment 2
Plaintext Segment 3
x = x1 x2 x3 x4 x5 x6 x7 x8 x9 x10 x11 x12
and